



vulnerability reporting made easy

On June 13th a security researcher published details of a security vulnerability in Impero Education Pro, along with a tool to exploit it, (rather than bringing it to our attention privately), something that as a business we do not condone. Following this incident, we have had a number of security researchers approach us to ask 'what is the best way to report these things?' so we hope that this statement helps to clarify things.

The following policy outlines how perceived security vulnerabilities can be reported to Impero efficiently:

<https://www.imperosoftware.co.uk/corporate/reporting-vulnerabilities/>

While we appreciate all methods of private disclosure (phone call, email, face-to-face meeting) some can be less efficient in processing the information. We had an incident last week where one security researcher turned up on our doorstep

armed with "over 9000" printed copies of a single suspected vulnerability and a chest-mounted Go Pro camera (sensibly capturing on record that this had been received!).

To save future cost, time and carbon footprint, should security researchers be contemplating similar methods, we wanted to make clear that an email to security@imperosoftware.com will suffice! This way there is an electronic audit of the information. A scan of the information submitted showed the vulnerability had already been reported through the usual channels and has been fixed in our August release. Unfortunately, as this researcher didn't leave his email address we have been unable to update him on the progress of this!

As always if anyone has any questions please get in touch.

